

Recipe 17 - Configuration Guide for Setting up Entegrity AssureAccess 3.0.0.4 as an AA and CS	
Table of Contents:	
1	Setup 1
1.1	Terms and Introduction 1
2	Partner Configuration 2
2.1	Open Entegrity for Configuration..... 2
2.2	Configure a Partner AA..... 3
2.3	Configure a Partner CS..... 8
Version 2.0.0	

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Entegrity AssureAccess 3.0.0.4 as an Agency Application (AA) and Credential Service (CS). Remember that the Entegrity AssureAccess setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the administration console screen shown in Figure 17-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

2 Partner Configuration

2.1 Open Entegrity for Configuration

Open the Entegrity AssureAccess Administration Console. The administration console screen should appear as shown in Figure 17-1. Next, click on the **SAMLsrc** toggle provided in the left-hand Domain View.

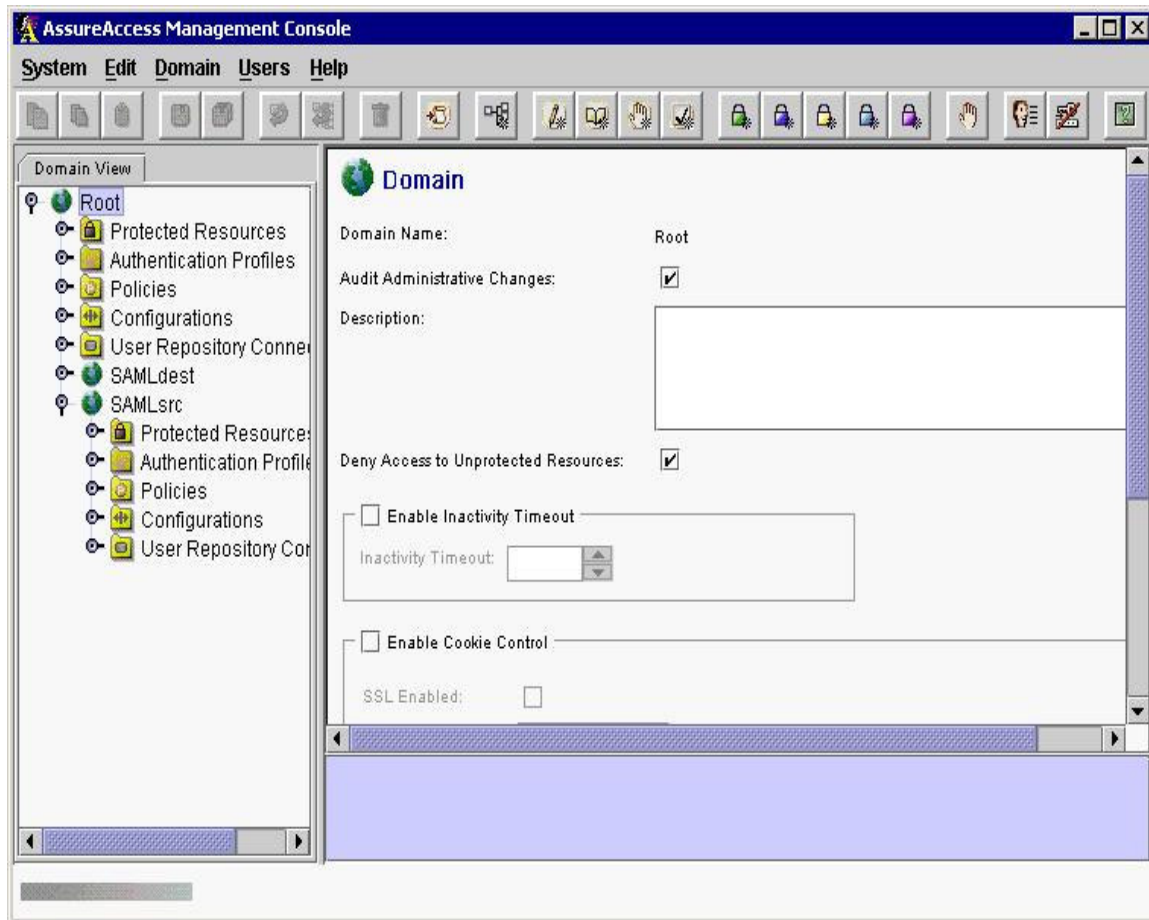


Figure 17-1: Administration Console Screen

2.2 Configure a Partner AA

Next, click on the **Configurations** toggle and then the **Web Adapter** option. The Web Adapter Configuration screen should appear as shown in Figure 17-2. Click on the **Add Mapping...** button.

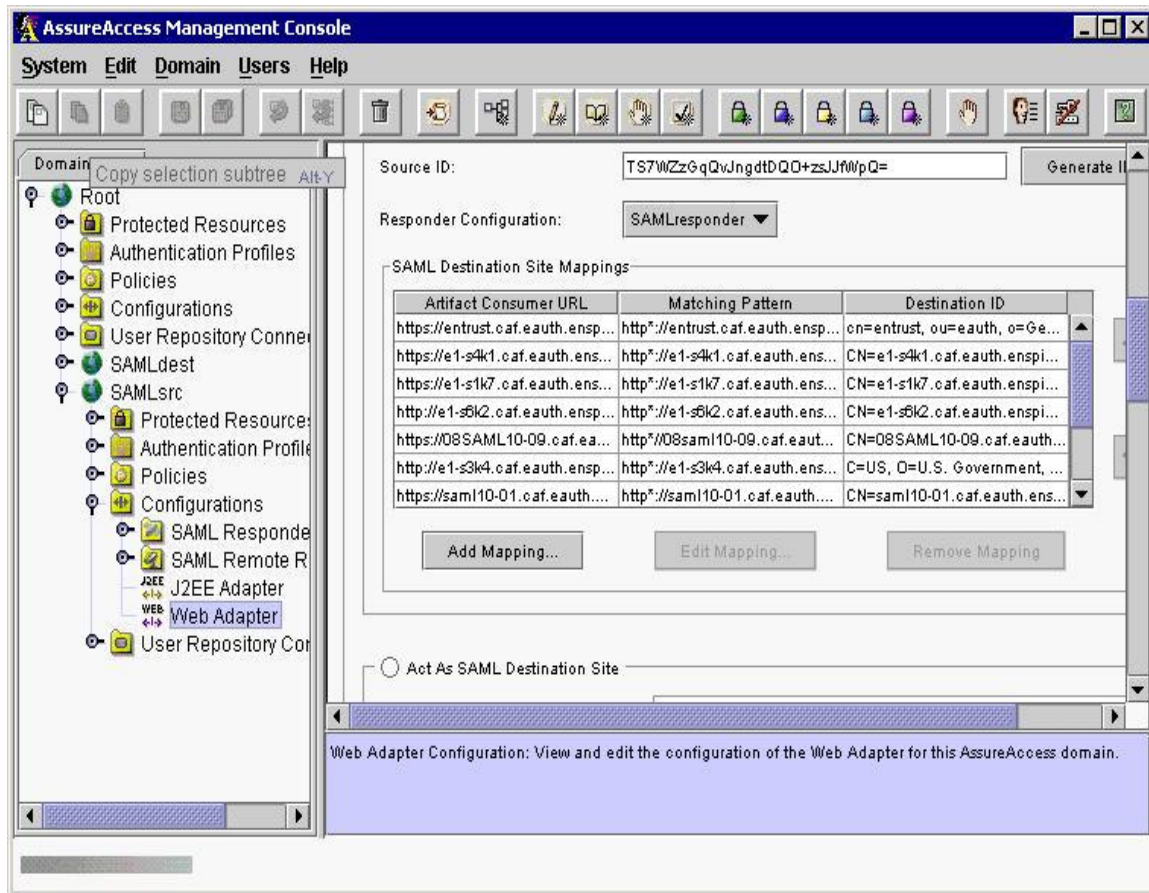
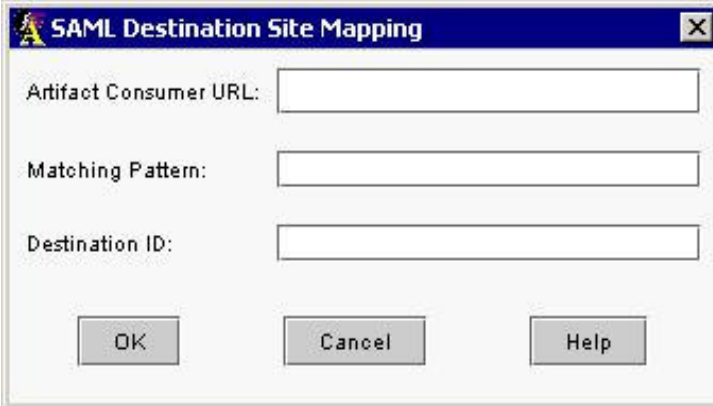


Figure 17-2: Web Adapter Configuration

Once you have selected the **Add Mapping...** button, the SAML Destination Site Mapping dialog box should appear as shown in Figure 17-3.



The image shows a Windows-style dialog box titled "SAML Destination Site Mapping". It has a blue title bar with a small icon on the left and a close button (X) on the right. The main area is white and contains three text input fields, each with a label to its left: "Artifact Consumer URL:", "Matching Pattern:", and "Destination ID:". Below these fields are three buttons: "OK", "Cancel", and "Help", arranged horizontally.

Figure 17-3: SAML Destination Site Mapping Dialog Box

As demonstrated in Figure 17-4, enter the **Artifact Receiver URL** in the **Artifact Consumer URL** field. Next, enter the **matching pattern** in the **Matching Pattern** field. This is the pattern that will map to this AA. Once those two steps are complete, enter the **Destination ID** in the **Destination ID** field and then select the **OK** button.



The image shows a Windows-style dialog box titled "SAML Destination Site Mapping". It contains three text input fields with labels to their left. The first field is labeled "Artifact Consumer URL:" and contains the text "https://www.newsite.com/artifact". The second field is labeled "Matching Pattern:" and contains the text "http*://www.newsite.com*/". The third field is labeled "Destination ID:" and contains the text "cn=Newsite App, ou=Some Agency, o=U.". At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Help".

Field Label	Field Value
Artifact Consumer URL:	https://www.newsite.com/artifact
Matching Pattern:	http*://www.newsite.com*/
Destination ID:	cn=Newsite App, ou=Some Agency, o=U.

Figure 17-4: Enter SAML Destination Site Mapping Information

Once the **OK** button has been selected, the SAML Destination Site Mapping screen should disappear. As demonstrated in Figure 17-5, right click on the **Web Adapter** toggle and then **Save**.

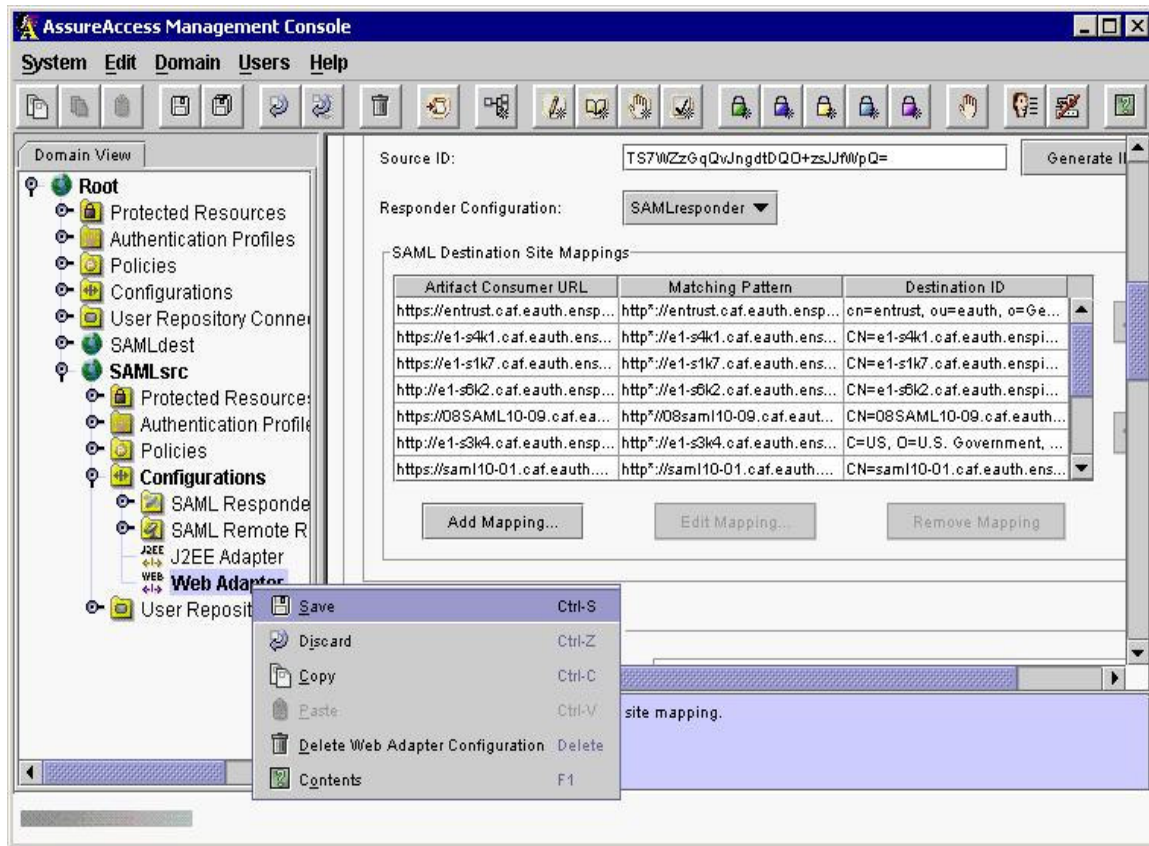


Figure 17-5: SAML Destination Site Mapping

Next, select **System** and then **Send Update** as shown in Figure 17-6.

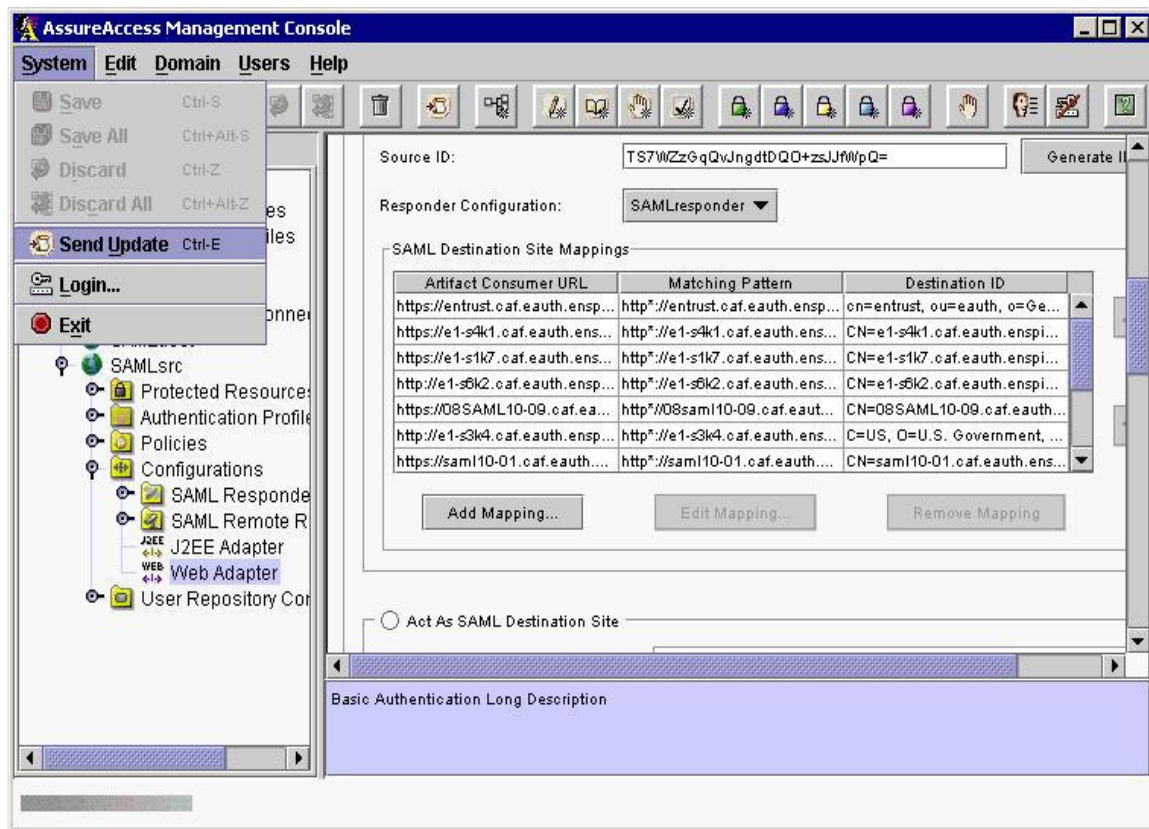


Figure 17-6: Send Update

2.3 Configure a Partner CS

First, open the Entegrity AssureAccess Administration Console as previously described (Figure 17-1). From the Administration Console screen, click on the **SAMLdest** and **Configurations** toggle and the Configurations screen will appear as shown in Figure 17-7. Next, click on the **SAML Remote Responders** toggle.

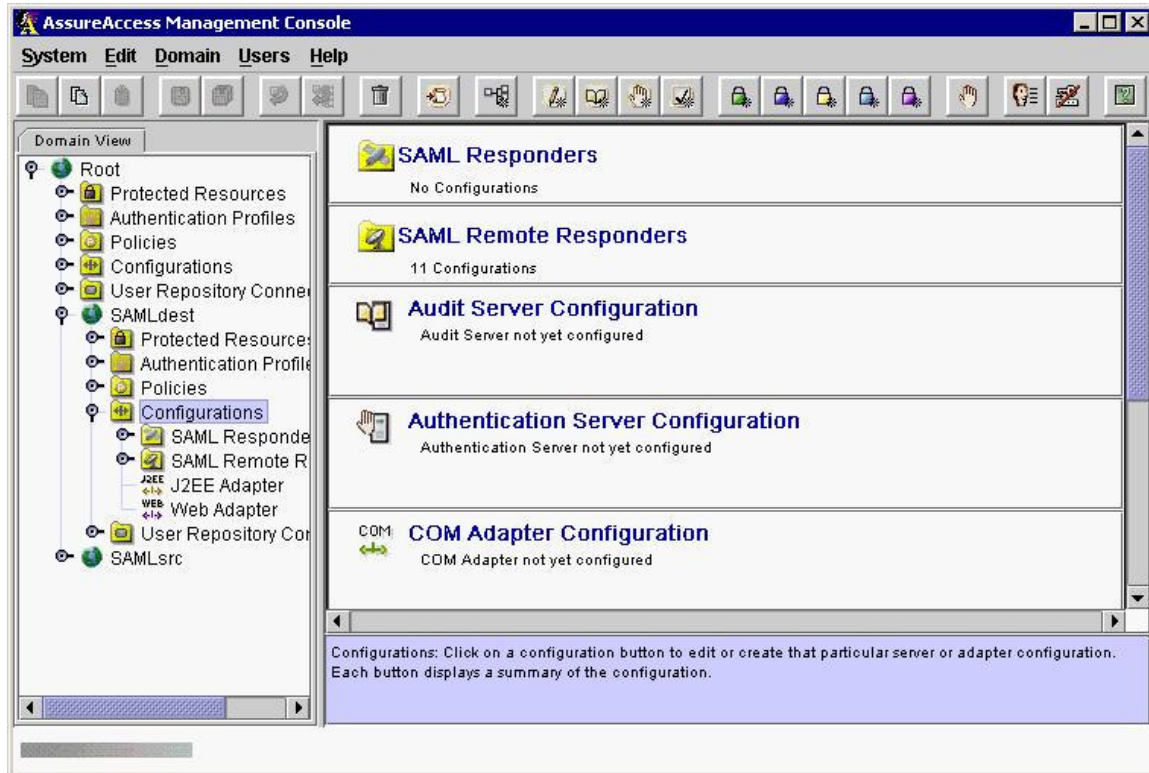


Figure 17-7: Configurations

Once the SAML Remote Responders toggle has been selected, the SAML Remote Responder screen should appear as shown in Figure 17-8.

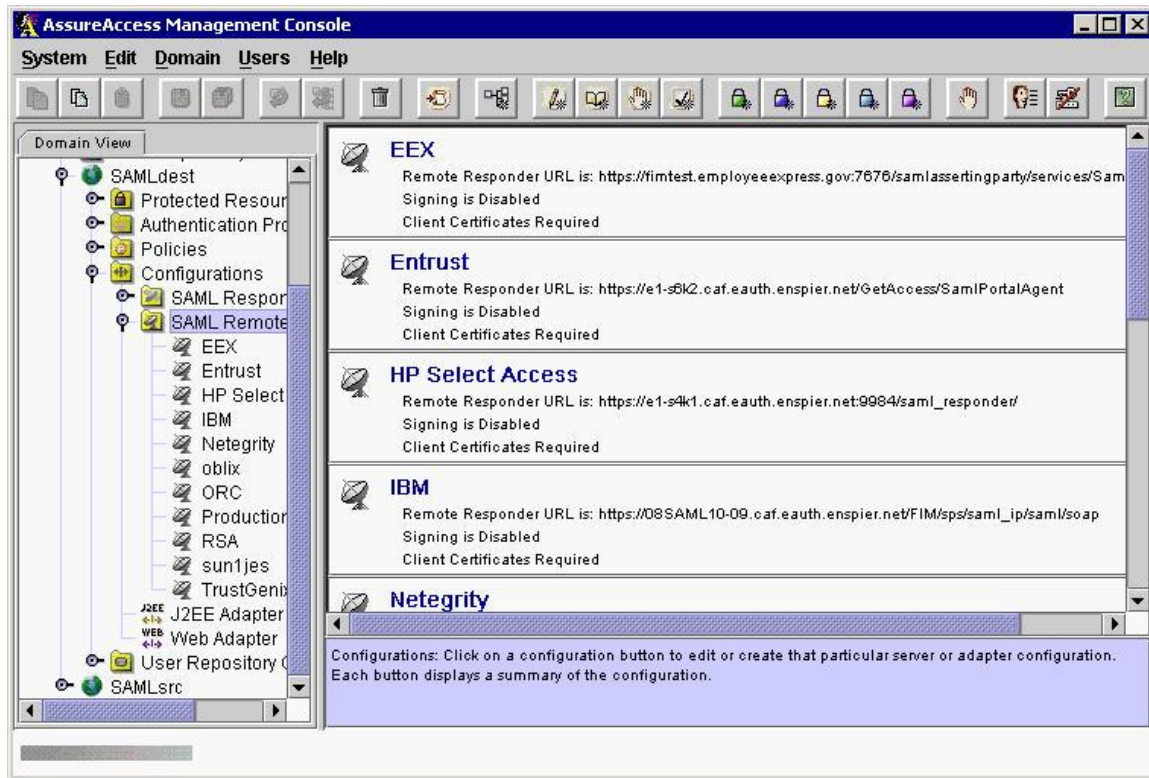


Figure 17-8: SAML Remote Responder

As demonstrated in Figure 17-9, right click on the **SAML Remote Responder** and then select **Create SAML Remote Responder Configuration**.

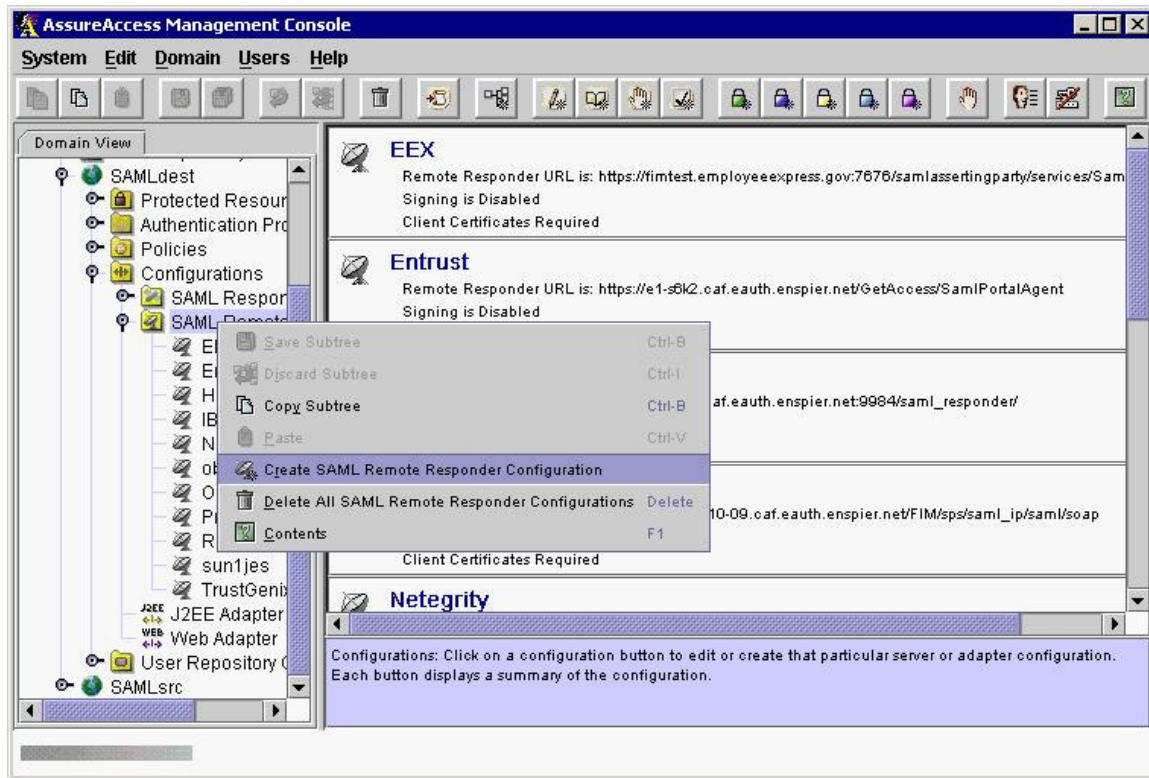


Figure 17-9: Create SAML Remote Responder Configuration

The SAML Remote Responder Configuration screen should appear as shown in Figure 17-10. Next, type a **name** for this configuration in the **SAML Remote Responder Name** field, type the **responder URL** in the **Remote Responder URL** field, and then select **Client Certificates** from the **Authentication Method** options.

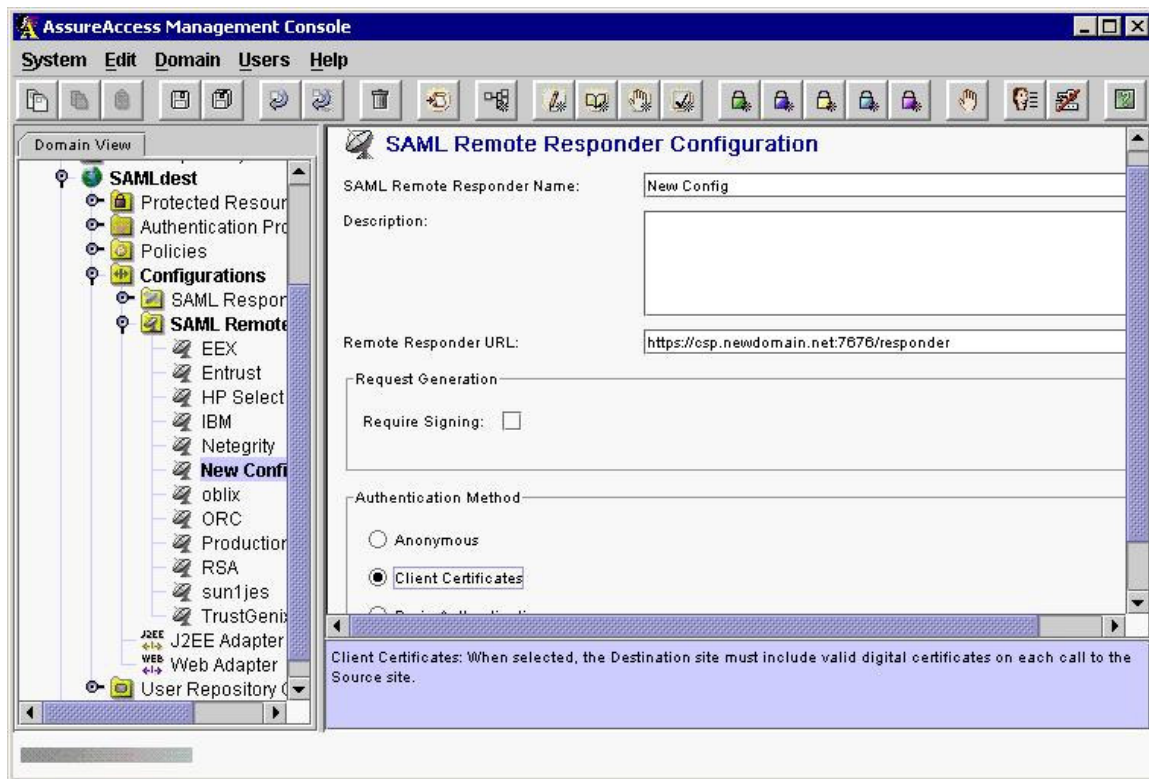


Figure 17-10: Enter SAML Remote Responder Configuration Information

As demonstrated in Figure 17-11, right click on **New Configuration** and select **Save**.

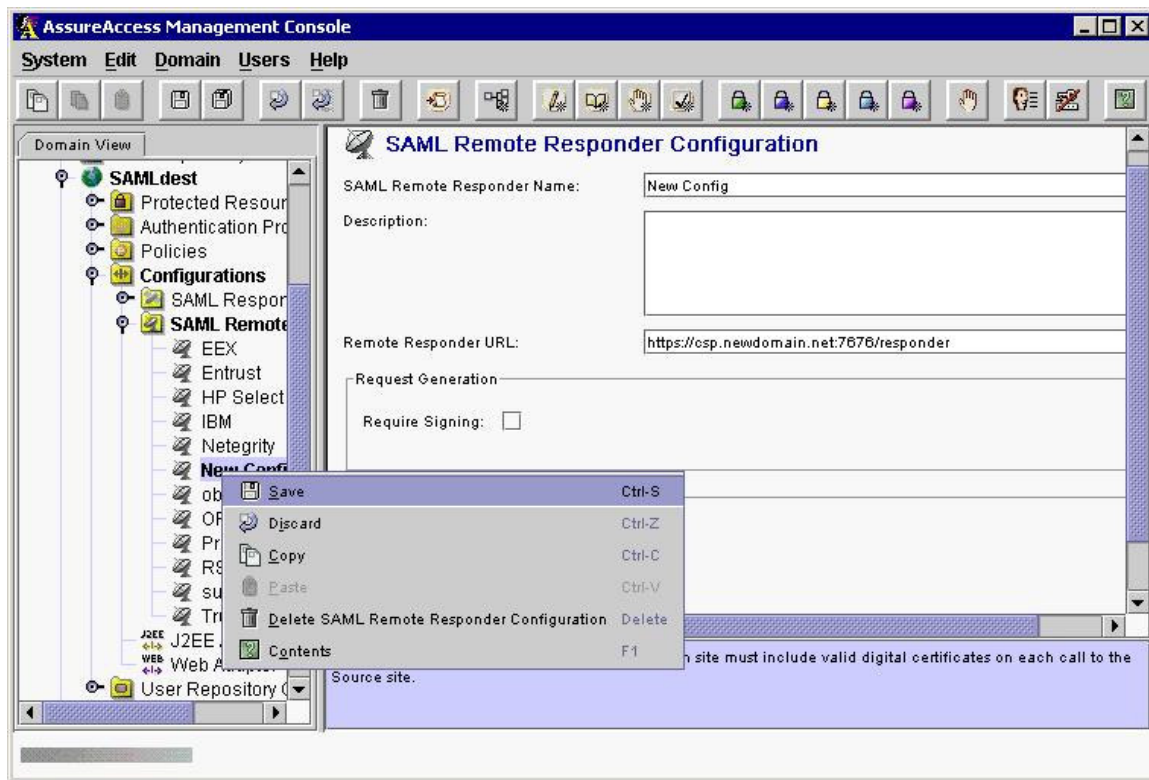


Figure 17-11: Save New Configuration

Next, click on **Web Adapter**. Once the Act As SAML Destination Site screen appears as shown in Figure 17-12, click on the **Add Mapping...** button.

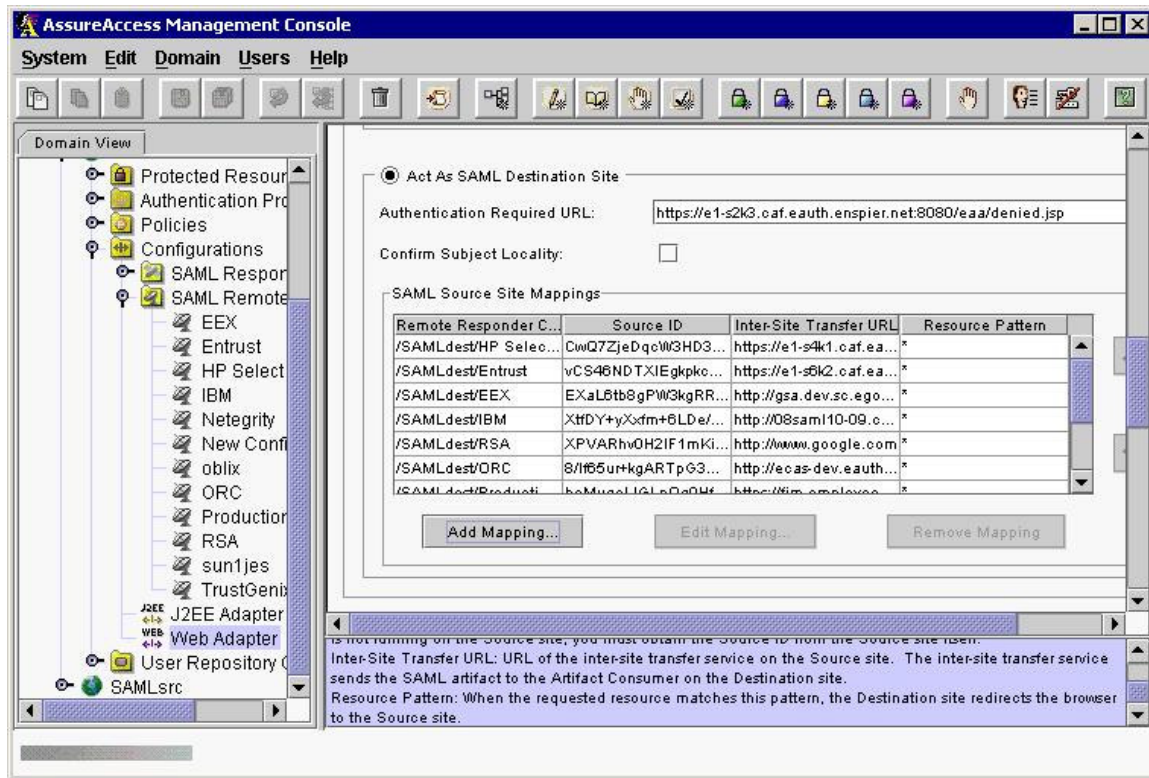
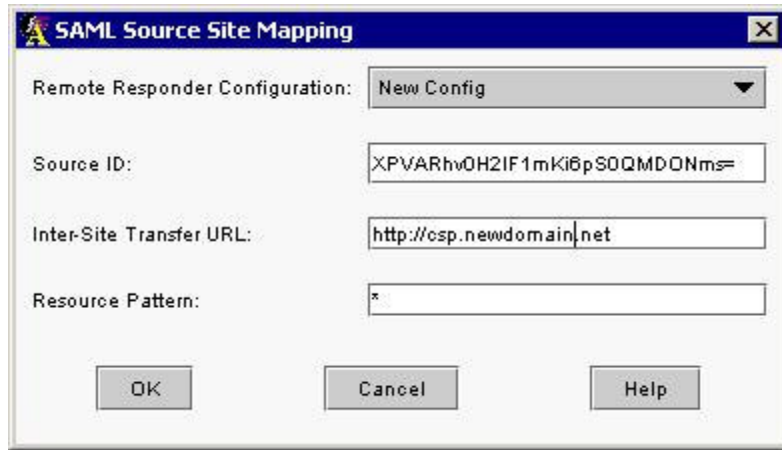


Figure 17-12: Act As SAML Destination Site

Once the **Add Mapping...** button has been selected, the SAML Source Site Mapping screen should appear as shown in Figure 17-13. Next, select the **name** of the previous configuration created in the **Remote Responder Configuration** drop down list, enter the **Source ID** in the **Source ID** field, enter any **valid URL** in the **Inter-Site Transfer URL** field, enter the **Resource Pattern** that users will be allowed to access in your application in the Resource Pattern field, and then select the **OK** button.



The image shows a Windows-style dialog box titled "SAML Source Site Mapping". It contains four input fields and three buttons at the bottom. The "Remote Responder Configuration" field is a dropdown menu currently showing "New Config". The "Source ID" field contains the text "XPVARhw0H2IF1mKi6pS0QMDONms=". The "Inter-Site Transfer URL" field contains "http://osp.newdomain.net". The "Resource Pattern" field contains an asterisk "*". The buttons at the bottom are "OK", "Cancel", and "Help".

Field Label	Value
Remote Responder Configuration:	New Config
Source ID:	XPVARhw0H2IF1mKi6pS0QMDONms=
Inter-Site Transfer URL:	http://osp.newdomain.net
Resource Pattern:	*

Figure 17-13: SAML Source Site Mapping

Once the SAML Source Site Mapping screen disappears, right click on **Web Adapter** and select **Save** as demonstrated in Figure 17-14.

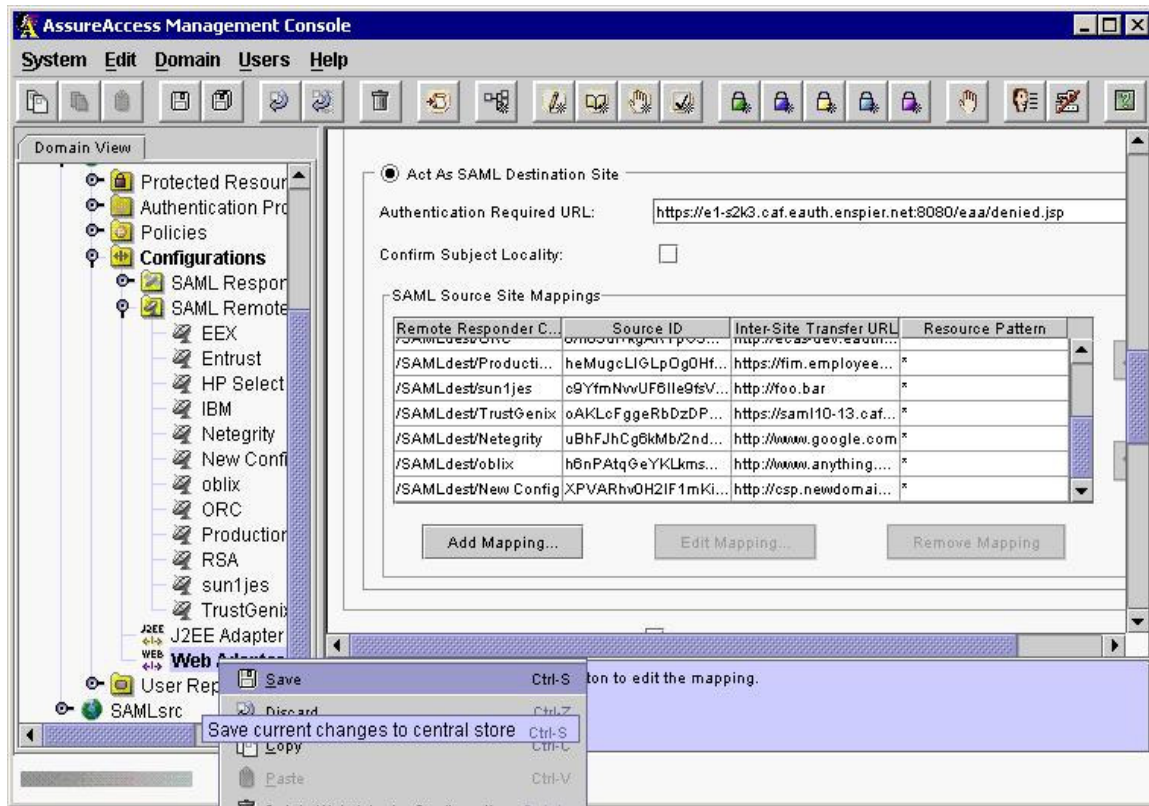


Figure 17-14: Save Web Adapter

Next, select **System** and then **Send Update** as shown in Figure 17-15.

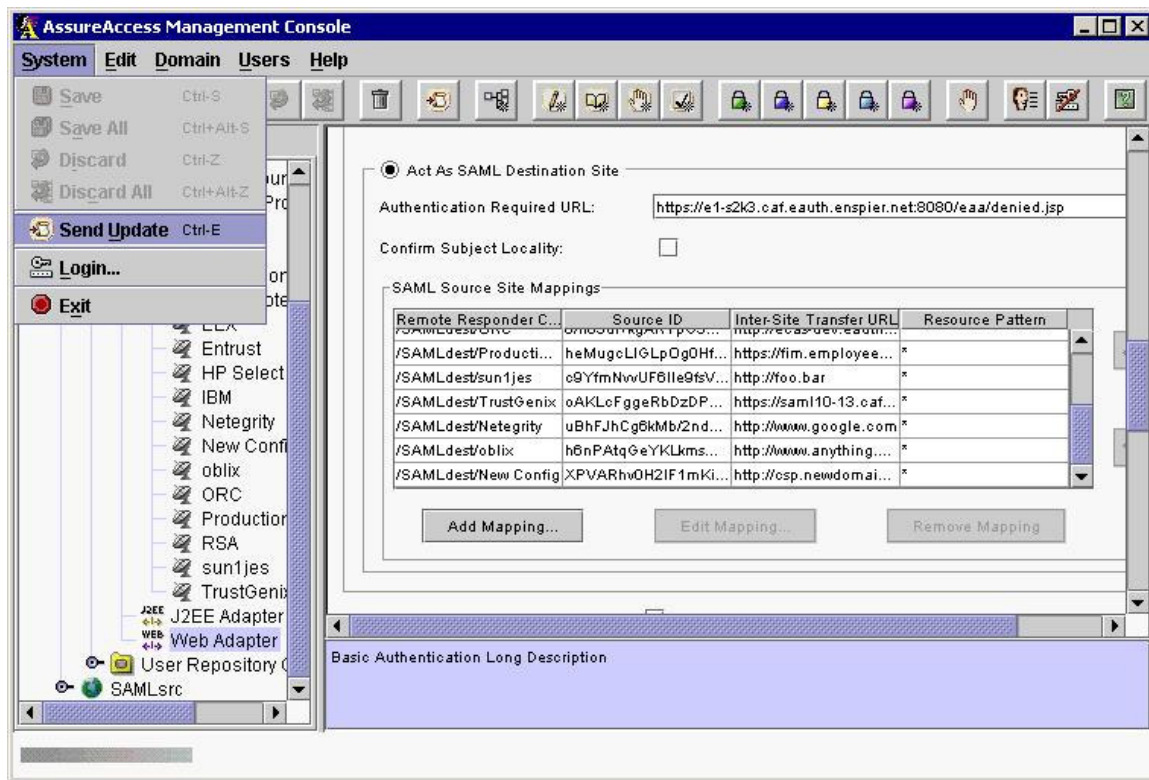


Figure 17-15: Send Update